UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/084,880 | 02/27/2002 | Nina Lewis | 255/221 | 7239 |

23639 7590 10/10/2006

BINGHAM, MCCUTCHEN LLP
THREE EMBARCADERO CENTER
18 FLOOR
SAN FRANCISCO, CA 94111-4067

| EXAMINER | |
|---|---|
| GANDHI, DIPAKKUMAR B | |
| **ART UNIT** | **PAPER NUMBER** |
| 2138 | |

DATE MAILED: 10/10/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/084,880 | LEWIS, NINA | |
| | Examiner | Art Unit | |
| | Dipakkumar Gandhi | 2138 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *11 August 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-51* is/are pending in the application.

4a) Of the above claim(s) *10 and 43* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9,11-42 and 44-51* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 February 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

***Response to Amendment***

1. Applicant's Request for Continued Examination (RCE) filed on 8/11/2006 and amendment after final filed on 7/11/2006 (including amended claims) have been entered.

2. Applicant's arguments with respect to claims 1, 19 and 39 have been considered but are moot in view of the new ground(s) of rejection.

***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

5. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cohen et al. (US 6,178,511 B1) in view of Moriconi et al. (US 6,158,010) and Franklin et al. (US 2001/0023440 A1).

As per claim 1, Cohen et al. teach a method for managing a method for managing user access information for access to one or more database network nodes, the method comprising: storing database user authentication information; receiving an access request from a user for the network node; authenticating the user based upon the database user authentication information (fig. 2, col. 4, lines 35-45, lines 61-67, col. 5, lines 16-40, Cohen et al.).

However Cohen et al. do not explicitly teach the specific use of storing database user authorization in a central directory that is connected to one or more databases, the database user authorization comprising a user role, the user role comprising one or more privileges; locally defining the

user role at a network node; granting the user privileges on the network node based upon the user role; wherein the database user authorization is stored as one or more data objects in the central directory.

Moriconi et al. in an analogous art teach that an authorization...directory servers (col. 6, line 33-col. 7, line 11, Moriconi et al.). Moriconi et al. also teach that a privilege...granted or denied to the role (col. 7, line 34-60, Moriconi et al.).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Cohen et al.'s patent with the teachings of Moriconi et al. by including an additional step of storing database user authorization in a central directory that is connected to one or more databases, the database user authorization comprising a user role, the user role comprising one or more privileges; locally defining the user role at a network node; granting the user privileges on the network node based upon the user role; wherein the database user authorization is stored as one or more data objects in the central directory.

This modification would have been obvious to one of ordinary skill in the art, at the time the invention was made, because one of ordinary skill in the art would have recognized that it would provide the opportunity to provide more security in protecting the data using different roles for different users.

Cohen et al. also do not explicitly teach specifically that one of the one or more data objects comprises a distinguished name that does not include a user name.

However Franklin et al. in an analogous art teach that a user object 98 is associated with an individual user. The distinguished name 144 of FIG. 6 is exemplary of all distinguished names 124. Each distinguished name 124 typically includes a common name 146 in association with a context 148. Context 148 may include acronyms, abbreviations, or other identifications of organizations, geography, logical relationships, and enterprises, as illustrated (fig. 5, 6, page 4, paragraph 53, Franklin et al.).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Cohen et al.'s patent with the teachings of Franklin et al. by including additionally that one of the one or more data objects comprises a distinguished name that does not include a user name.

This modification would have been obvious to one of ordinary skill in the art, at the time the invention was made, because one of ordinary skill in the art would have recognized that one of the one or more data objects comprising a distinguished name that does not include a user name would provide the opportunity to associate a user object with an individual user.

6. Claims 2-4, 11, 12, 13, 14, 15, 16, 17, 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cohen et al. (US 6,178,511 B1), Moriconi et al. (US 6,158,010) and Franklin et al. (US 2001/0023440 A1) as applied to claim 1 above, and further in view of Ferguson et al. (US 2002/0082818 A1).

As per claim 2, Cohen et al., Moriconi et al. and Franklin et al. substantially teach the claimed invention described in claim 1 (as rejected above).

However Cohen et al., Moriconi et al. and Franklin et al. do not explicitly teach the specific use of an LDAP-compatible directory.

Ferguson et al. in an analogous art teach that this is accomplished by user authentication via a lightweight directory access protocol (LDAP) server that authenticates users within particular domain names that map to specific customer accounts (page 4, paragraph 41, Ferguson et al.).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Cohen et al.'s patent with the teachings of Ferguson et al. by including an additional step of using an LDAP-compatible directory.

This modification would have been obvious to one of ordinary skill in the art, at the time the invention was made, because one of ordinary skill in the art would have recognized that using an LDAP-compatible directory would provide the opportunity to use a hierarchical structure for user authentication during login process.

- As per claim 3, Cohen et al., Moriconi et al., Franklin et al. and Ferguson et al. teach the additional limitations.

Ferguson et al. teach the method in which the database user authentication information is stored at the central directory (page 4, paragraph 41, Ferguson et al.).

- As per claim 4, Cohen et al., Moriconi et al., Franklin et al. and Ferguson et al. teach the additional limitations.

Ferguson et al. teach the method in which the database user authorization is stored in a schema having a hierarchy of schema objects (page 4, paragraph 41, Ferguson et al.).

- As per claim 11, Cohen et al., Moriconi et al., Franklin et al. and Ferguson et al. teach the additional limitations.

Ferguson et al. teach the method in which the one or more objects are stored in a security subtree in the central directory (figure 1, page 3, paragraph 36, Ferguson et al.).

- As per claim 12, Cohen et al., Moriconi et al., Franklin et al. and Ferguson et al. teach the additional limitations.

Ferguson et al. teach the method in which administrative access is controlled to one or more data objects in the central directory (page 25, paragraph 196, Ferguson et al.)

- As per claim 13, Cohen et al., Moriconi et al., Franklin et al. and Ferguson et al. teach the additional limitations.

Ferguson et al. teach the method in which access control is implemented using an access control point associated with the one or more data objects in the central directory (page 19, paragraph 150, Ferguson et al.).

- As per claim 14, Cohen et al., Moriconi et al., Franklin et al. and Ferguson et al. teach the additional limitations.

Ferguson et al. teach the method in which the access control point is associated with access policies for a subtree of the one or more database objects in the central directory (page 19, paragraph 145, Ferguson et al.).

- As per claim 15, Cohen et al., Moriconi et al., Franklin et al. and Ferguson et al. teach the additional limitations.

Ferguson et al. teach the method in which the access control point is associated with access policies for a single entry for the one or more database objects in the central directory (page 19, paragraph 145, Ferguson et al.).

- As per claim 16, Cohen et al., Moriconi et al., Franklin et al. and Ferguson et al. teach the additional limitations.

Ferguson et al. teach the method in which the access control point is associated with individually named users (page 18-19, paragraph 144-145, Ferguson et al.).

- As per claim 17, Cohen et al., Moriconi et al., Franklin et al. and Ferguson et al. teach the additional limitations.

Ferguson et al. teach the method in which the access control point is associated with a group of users (page 18-19, paragraph 144-145, Ferguson et al.).

- As per claim 18, Cohen et al., Moriconi et al., Franklin et al. and Ferguson et al. teach the additional limitations.

Ferguson et al. teach the method in which members of the group are associated with a set of access privileges associated with the access control point (page 19, paragraph 145, 152, Ferguson et al.).

7. Claims 5-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cohen et al. (US 6,178,511 B1), Moriconi et al. (US 6,158,010), Franklin et al. (US 2001/0023440 A1) and Ferguson et al. (US 2002/0082818 A1) as applied to claim 4 above, and further in view of Gavrila et al. (US 2002/0026592 A1).

As per claim 5, Cohen et al., Moriconi et al., Franklin et al. and Ferguson et al. substantially teach the claimed invention described in claim 4 (as rejected above).

However Cohen et al., Moriconi et al., Franklin et al. and Ferguson et al. do not explicitly teach the specific use of the method in which the hierarchy of schema objects comprises an enterprise role, wherein the enterprise role is associated with one or more users and one or more locally defined roles.

Gavrila et al. in an analogous art teach that this invention makes use, in yet a further aspect, of both local and global groups for the instantiation of roles on multiple computer hosts, to implement nested groups and to enable the integration of extant host computers, which include local user accounts and groups defined on independent servers and workstations, within large distributed operating systems (abstract, Gavrila et al.).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Cohen et al.'s patent with the teachings of Gavrila et al by including an additional step of using the method in which the hierarchy of schema objects comprises an enterprise role, wherein the enterprise role is associated with one or more users and one or more locally defined roles.

This modification would have been obvious to one of ordinary skill in the art, at the time the invention was made, because one of ordinary skill in the art would have recognized that it would provide the opportunity to define a global role to associate the users with the authorization to access local databases.

- As per claim 6, Cohen et al., Moriconi et al., Franklin et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Gavrila et al. teach that the privileges associated with the one or more locally defined roles are assigned to the one or more users (abstract, page 3, paragraph 22, Gavrila et al.).

- As per claim 7, Cohen et al., Moriconi et al., Franklin et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Gavrila et al. teach the method in which the hierarchy of schema objects comprises an enterprise domain, wherein the enterprise domain comprises one or more enterprise roles (page 2, paragraph 10, Gavrila et al.).

- As per claim 8, Cohen et al., Moriconi et al., Franklin et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Gavrila et al. teach the method in which each of the one or more enterprise roles is associated with one or more users and one or more locally defined roles (abstract, Gavrila et al.).

- As per claim 9, Cohen et al., Moriconi et al., Franklin et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Gavrila et al. teach the method in which the enterprise domain is associated with one or more network nodes (page 3, paragraph 22, Gavrila et al.).

8. Claims 19-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cohen et al. (US 6,178,511 B1) in view of Moriconi et al. (US 6,158,010), Franklin et al. (US 2001/0023440 A1), Ferguson et al. (US 2002/0082818 A1) and Gavrila et al. (US 2002/0026592 A1).

As per claim 19, Cohen et al. teach a system for managing user access information for one or more database network nodes, comprising: one or more database network nodes for which user access is sought; and the user access information data objects comprising authentication (fig. 2, col. 4, lines 35-45, lines 61-67, col. 5, lines 16-40, Cohen et al.).

However Cohen et al. do not explicitly teach the specific use of a LDAP directory and user access information data objects stored in the LDAP directory.

Ferguson et al. in an analogous art teach that this is accomplished by user authentication via a lightweight directory access protocol (LDAP) server that authenticates users within particular domain names that map to specific customer accounts (page 4, paragraph 41, Ferguson et al.).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Cohen et al.'s patent with the teachings of Ferguson et al. by including an additional step of using a LDAP directory and user access information data objects stored in the LDAP directory.

This modification would have been obvious to one of ordinary skill in the art, at the time the invention was made, because one of ordinary skill in the art would have recognized that using a LDAP directory and user access information data objects stored in the LDAP directory would provide the opportunity to use a hierarchical structure for user authentication during login process.

Cohen et al. also do not explicitly teach the specific use of the user access information data objects comprising authorization information, wherein the authorization information is associated with a scope of access for a user.

However Moriconi et al. in an analogous art teach that an authorization...directory servers (col. 6, line 33-col. 7, line 11, Moriconi et al.). Moriconi et al. also teach that a privilege...granted or denied to the role (col. 7, line 34-60, Moriconi et al.).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Cohen et al.'s patent with the teachings of Moriconi et al. by including an additional step of using the user access information data objects comprising authorization information, wherein the authorization information is associated with a scope of access for a user.

This modification would have been obvious to one of ordinary skill in the art, at the time the invention was made, because one of ordinary skill in the art would have recognized that it would provide the opportunity to provide more security in protecting the data using scope of access for different users.

Cohen et al. also do not explicitly teach specifically that the user access information data objects are associated with an enterprise role, the enterprise role comprising a collection of roles associated with one or more databases.

However Gavrila et al. in an analogous art teach local and global groups for the instantiation of roles on multiple computer hosts (abstract, Gavrila et al.). Gavrila et al. also teach role instances of a role on a host computer or set of host computers...both instances were derived on the same set of host computers (page 3, paragraph 22, Gavrila et al.).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Cohen et al.'s patent with the teachings of Gavrila et al. by including an additional step of using the user access information data objects associated with an enterprise role, the enterprise role comprising a collection of roles associated with one or more databases.

This modification would have been obvious to one of ordinary skill in the art, at the time the invention was made, because one of ordinary skill in the art would have recognized that it would provide the opportunity to define a global role to associate the users with the authorization to access local databases.

Cohen et al. also do not explicitly teach specifically that one of the data objects comprises a distinguished name that does not include a user name.

However Franklin et al. in an analogous art teach that a user object 98 is associated with an individual user. The distinguished name 144 of FIG. 6 is exemplary of all distinguished names 124. Each distinguished name 124 typically includes a common name 146 in association with a context 148. Context 148 may include acronyms, abbreviations, or other identifications of organizations, geography, logical relationships, and enterprises, as illustrated (fig. 5, 6, page 4, paragraph 53, Franklin et al.).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Cohen et al.'s patent with the teachings of Franklin et al. by including additionally that one of data objects comprises a distinguished name that does not include a user name.

This modification would have been obvious to one of ordinary skill in the art, at the time the invention was made, because one of ordinary skill in the art would have recognized that one of the data objects comprising a distinguished name that does not include a user name would provide the opportunity to associate a user object with an individual user.

- As per claim 20, Cohen et al., Moriconi et al., Franklin et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Gavrila et al. teach the system in which the user access information data objects comprise a domain object that is associated with the one or more database network nodes (page 8, paragraph 98-99, Gavrila et al.).

- As per claim 21, Cohen et al., Moriconi et al., Franklin et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Gavrila et al. teach the system in which the domain object is associated with the enterprise role (page 8, paragraph 99, Gavrila et al.).

- As per claim 22, Cohen et al., Moriconi et al., Franklin et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Gavrila et al. teach the system in which the enterprise role is associated with a local database role (abstract, page 3, paragraph 22, Gavrila et al.).

- As per claim 23, Cohen et al., Moriconi et al., Franklin et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Gavrila et al. teach the system in which the scope of the local database role is locally defined at a local database network node (page 3, paragraph 22, Gavrila et al.).

Ferguson et al. teach database (page 4, paragraph 41, Ferguson et al.).

- As per claim 24, Cohen et al., Moriconi et al., Franklin et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Gavrila et al. teach the system in which the enterprise role is associated with one more users (page 3, paragraph 22, Gavrila et al.).

- As per claim 25, Cohen et al., Moriconi et al., Franklin et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Gavrila et al. teach the system in which each of the one or more users is associated with privileges defined for the enterprise role (abstract, page 3, paragraph 22, Gavrila et al.).

- As per claim 26, Cohen et al., Moriconi et al., Franklin et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Ferguson et al. teach the system in which the user access information data objects comprise an access control point attribute (page 18-19, paragraph 144-145, Ferguson et al.).

- As per claim 27, Cohen et al., Moriconi et al., Franklin et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Ferguson et al. teach the system in which the access control point attribute is established only if access control policies are established for a corresponding object (page 19, paragraph 145, Ferguson et al.).

- As per claim 28, Cohen et al., Moriconi et al., Franklin et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Ferguson et al. teach the system in which the access control point attribute is associated with access policies for a subtree in the user access information data objects stored in the LDAP directory (page 19, paragraph 145, Ferguson et al.).

- As per claim 29, Cohen et al., Moriconi et al., Franklin et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Ferguson et al. teach the system in which the access control point attribute is associated with access policies for a single entry in the user access information data objects stored in the LDAP directory (page 19, paragraph 145, Ferguson et al.).

- As per claim 30, Cohen et al., Moriconi et al., Franklin et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Ferguson et al. teach the system in which the access control point attribute is associated with individually named users (page 18-19, paragraph 144-145, Ferguson et al.).

- As per claim 31, Cohen et al., Moriconi et al., Franklin et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Ferguson et al. teach the system in which the access control point attribute is associated with a group of users (page 18-19, paragraph 144-145, Ferguson et al.).

- As per claim 32, Cohen et al., Moriconi et al., Franklin et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Ferguson et al. teach the system in which members of the group are associated with a set of access privileges associated with the access control (page 18-19, paragraph 144-145, Ferguson et al.).

- As per claim 33, Cohen et al., Moriconi et al., Franklin et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Ferguson et al. teach the system in which the user access information data objects comprise a mapping object that maps a database user to a database schema (page 4, paragraph 41, Ferguson et al.).

- As per claim 34, Cohen et al., Moriconi et al., Franklin et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Ferguson et al. teach the system in which the mapping object affects a single user (page 4, paragraph 41, Ferguson et al.).

- As per claim 35, Cohen et al., Moriconi et al., Franklin et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Ferguson et al. teach the system in which the mapping object is associated with a full distinguished name (page 4, paragraph 41, Ferguson et al.).

- As per claim 36, Cohen et al., Moriconi et al., Franklin et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Ferguson et al. teach the system in which the mapping object is associated with a plurality of users (page 4, paragraph 41, Ferguson et al.).

- As per claim 37, Cohen et al., Moriconi et al., Franklin et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Ferguson et al. teach the system in which the mapping object is associated with a partial distinguished name (page 4, paragraph 41, Ferguson et al.).

- As per claim 38, Cohen et al., Moriconi et al., Franklin et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Gavrila et al. teach the system in which the enterprise role is associated with local database roles from a plurality of database nodes (abstract, Gavrila et al.).

9. Claim 39 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cohen et al. (US 6,178,511 B1) in view of Moriconi et al. (US 6,158,010), Franklin et al. (US 2001/0023440 A1) and Gavrila et al. (US 2002/0026592 A1).

As per claim 39, Cohen et al. teach a process for managing user access information for database network nodes, the process comprising: storing database user authentication information; receiving an access request from a user for the network node and authenticating the user based upon the database user authentication information (fig. 2, col. 4, lines 35-45, lines 61-67, col. 5, lines 16-40, Cohen et al.).

However Cohen et al. do not explicitly teach the specific use of storing database user authorization in a central directory that is connected to one or more databases, the database user authorization comprising a user role, the user role comprising one or more privileges; locally defining the user role at a network node; granting the user privileges on the network node based upon the user role; wherein the database user authorization is stored as one or more data objects in the central directory.

Moriconi et al. in an analogous art teach that an authorization...directory servers (col. 6, line 33-col. 7, line 11, Moriconi et al.). Moriconi et al. also teach that a privilege...granted or denied to the role (col. 7, line 34-60, Moriconi et al.).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Cohen et al.'s patent with the teachings of Moriconi et al. by including an additional step of storing database user authorization in a central directory that is connected to one or more databases, the database user authorization comprising a user role, the user role comprising one or more

privileges; locally defining the user role at a network node; granting the user privileges on the network node based upon the user role; wherein the database user authorization is stored as one or more data objects in the central directory.

This modification would have been obvious to one of ordinary skill in the art, at the time the invention was made, because one of ordinary skill in the art would have recognized that it would provide the opportunity to provide more security in protecting the data using different roles for different users.

Cohen et al. also do not explicitly teach specifically that one of the one or more data objects comprises a distinguished name that does not include a user name.

However Franklin et al. in an analogous art teach that a user object 98 is associated with an individual user. The distinguished name 144 of FIG. 6 is exemplary of all distinguished names 124. Each distinguished name 124 typically includes a common name 146 in association with a context 148. Context 148 may include acronyms, abbreviations, or other identifications of organizations, geography, logical relationships, and enterprises, as illustrated (fig. 5, 6, page 4, paragraph 53, Franklin et al.).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Cohen et al.'s patent with the teachings of Franklin et al. by including additionally that one of the one or more data objects comprises a distinguished name that does not include a user name.

This modification would have been obvious to one of ordinary skill in the art, at the time the invention was made, because one of ordinary skill in the art would have recognized that one of the one or more data objects comprising a distinguished name that does not include a user name would provide the opportunity to associate a user object with an individual user.

Cohen et al. also do not explicitly teach the specific use of a computer program product that includes a medium usable by a processor, the medium having stored thereon a sequence of instructions which, when executed by said processor, causes said processor to execute a process.

However Gavrila et al. in an analogous art teach a computer program product containing computer readable code for causing a machine to perform the method (page 19, claim 22, Gavrila et al.).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Cohen et al.'s patent with the teachings of Gavrila et al. by including an additional step of using a computer program product that includes a medium usable by a processor, the medium having stored thereon a sequence of instructions which, when executed by said processor, causes said processor to execute a process.

This modification would have been obvious to one of ordinary skill in the art, at the time the invention was made, because one of ordinary skill in the art would have recognized that using a computer program product that includes a medium usable by a processor, the medium having stored thereon a sequence of instructions which, when executed by said processor, causes said processor to execute a process would provide the opportunity to execute the process faster and accurately.

10. Claims 40-42, 44-51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cohen et al. (US 6,178,511 B1), Moriconi et al. (US 6,158,010), Franklin et al. (US 2001/0023440 A1) and Gavrila et al. (US 2002/0026592 A1) as applied to claim 39 above, and further in view of Ferguson et al. (US 2002/0082818 A1).

As per claim 40, Cohen et al., Moriconi et al., Franklin et al. and Gavrila et al. substantially teach the claimed invention described in claim 39 (as rejected above).

However Cohen et al., Moriconi et al., Franklin et al. and Gavrila et al. do not explicitly teach the specific use of the central directory comprising an LDAP-compatible directory.

Ferguson et al. in an analogous art teach that this is accomplished by user authentication via a lightweight directory access protocol (LDAP) server that authenticates users within particular domain names that map to specific customer accounts (page 4, paragraph 41, Ferguson et al.).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Cohen et al.'s patent with the teachings of Ferguson et al. by including an additional step of using the central directory comprising an LDAP-compatible directory.

This modification would have been obvious to one of ordinary skill in the art, at the time the invention was made, because one of ordinary skill in the art would have recognized that using the central directory

comprising an LDAP-compatible directory would provide the opportunity to use a hierarchical structure for user authentication during login process.

- As per claim 41, Cohen et al., Moriconi et al., Franklin et al., Gavrila et al. and Ferguson et al. teach the additional limitations.

Ferguson et al. teach that the database user authentication information is stored at the central directory (page 4, paragraph 41, Ferguson et al.).

- As per claim 42, Cohen et al., Moriconi et al., Franklin et al., Gavrila et al. and Ferguson et al. teach the additional limitations.

Ferguson et al. teach that the database user authorization is stored in a schema having a hierarchy of schema objects (page 4, paragraph 41, Ferguson et al.).

- As per claim 44, Cohen et al., Moriconi et al., Franklin et al., Gavrila et al. and Ferguson et al. teach the additional limitations.

Ferguson et al. teach that the one or more objects are stored in a security subtree in the central directory (figure 1, page 3, paragraph 36, Ferguson et al.).

- As per claim 45, Cohen et al., Moriconi et al., Franklin et al., Gavrila et al. and Ferguson et al. teach the additional limitations.

Ferguson et al. teach that administrative access is controlled to one or more data objects in the central directory (page 25, paragraph 196, Ferguson et al.).

- As per claim 46, Cohen et al., Moriconi et al., Franklin et al., Gavrila et al. and Ferguson et al. teach the additional limitations.

Ferguson et al. teach that access control is implemented using an access control point associated with the one or more data objects in the central directory (page 19, paragraph 150, Ferguson et al.).

- As per claim 47, Cohen et al., Moriconi et al., Franklin et al., Gavrila et al. and Ferguson et al. teach the additional limitations.

Ferguson et al. teach that the access control point is associated with access policies for a subtree of the one or more database objects in the central directory (page 19, paragraph 145, Ferguson et al.).

- As per claim 48, Cohen et al., Moriconi et al., Franklin et al., Gavrila et al. and Ferguson et al. teach the additional limitations.

Ferguson et al. teach that the access control point is associated with access policies for a single entry for the one or more database objects in the central directory (page 19, paragraph 145, Ferguson et al.).

- As per claim 49, Cohen et al., Moriconi et al., Franklin et al., Gavrila et al. and Ferguson et al. teach the additional limitations.

Ferguson et al. teach that the access control point is associated with individually named users (page 18-19, paragraph 144-145, Ferguson et al.).

- As per claim 50, Cohen et al., Moriconi et al., Franklin et al., Gavrila et al. and Ferguson et al. teach the additional limitations.

Ferguson et al. teach that the access control point is associated with a group of users (page 18-19, paragraph 144-145, Ferguson et al.).

- As per claim 51, Cohen et al., Moriconi et al., Franklin et al., Gavrila et al. and Ferguson et al. teach the additional limitations.

Ferguson et al. teach that members of the group are associated with a set of access privileges associated with the access control point (page 19, paragraph 145, 152, Ferguson et al.).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Dipakkumar Gandhi whose telephone number is 571-272-3822. The examiner can normally be reached on 8:30 AM - 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on (571) 272-3819. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Dipakkumar Gandhi

Patent Examiner